UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

CIPHERBLADE, LLC, a Pennsylvania Limited Liability Corporation

PLAINTIFF,

v.

CIPHERBLADE, LLC, an Alaska Limited Liability Corporation, MANUEL KRIZ, MICHAEL KRAUSE, JORN HENRIK BERNHARD JANSSEN, SERGIO GARCIA, JUSTIN MAILE, IOANA VIDRASAN,

and

CIPHERBLADE APAC PTE LTD, a Singapore limited company, JUSSI AITTOLA,

and

OMEGA3ZONE GLOBAL LTD, a Cyprus limited company, PAUL MARNITZ,

and

INQUISITA SOLUTIONS LTD., a Cyprus limited company,

and

GREEN STONE BUSINESS ADVISORY FZ LLC, a United Arab Emirates Limited Liability Corporation.

DEFENDANTS.

Case No. 1:23-cv-05671-AKH

PLAINTIFF'S BRIEF IN SUPPORT OF APPLICATION FOR A TEMPORARY RESTRAINING ORDER, PRESERVATION ORDER, EXPEDITED DISCOVERY, AN ALTERNATIVE SERVICE ORDER, AND AN ORDER TO SHOW CAUSE SCHEDULING PRELIMINARY INJUNCTION MOTION

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

I. INTRODUCTION

Plaintiff CipherBlade LLC ("CipherBlade PA") was founded by Richard Sanders and is a leading firm in the burgeoning field of cryptocurrency loss investigations and related expert witness testimony. The gravamen of Plaintiff's claims is theft. Defendants stole and have denied Plaintiff access to CipherBlade PA's domain and the information technology infrastructure attributed to it such as its work email, its website, and the customer relationship management software containing Plaintiff's proprietary commercial information on customers, customer leads, ongoing matters, work product and pricing. Accordingly, Plaintiff now finds itself locked out of its own systems, denied access to its client information and work product and with no means to communicate with clients through its work email systems. Further, Defendants have made materially false and misleading statements on the website they converted from Plaintiff and now control, falsely attributing to themselves the investigative experience, credentials, expert witness experience, expertise and the investigative tools of Plaintiff. Clients have been and will continue to be misled, including confusion among clients who believe they are retaining or paying Plaintiff and its representatives when they are instead hiring Defendants. Plaintiff faces irreparable harm each day it is locked out of its systems, each day Defendants use those systems and the trade secrets they contain to unfairly compete, and each day Defendants make false statements attributing to them Plaintiff's credentials, investigative tools and investigative and expert witness experience.

The theft began surreptitiously but in earnest in February 2023 when CipherBlade PA's founder and Principal, Richard Sanders, took a step back from the day-to-day operations of the company to volunteer in Ukraine assisting the Ukrainian National Police with investigations involving cryptocurrency. Defendants' scheme included using material misrepresentations to take control of Mr. Sanders' email and other critical accounts, including Plaintiff's domain, thereby

gaining access to sensitive corporate information and Plaintiff's technology infrastructure. In doing so, Defendants obtained control over Plaintiff's most critical trade secrets concerning business operations, investigative protocols, investigative tools, customer agreements, ongoing confidential customer matters, pricing, and confidential customer leads. Their theft included more commonplace asset diversions too. Defendants used their access and creation of fraudulent entities to convert digital cryptocurrency assets and funds in U.S. dollars and euros from Plaintiff's corporate accounts, to convert accounts receivable, and to convert clients, client leads. Defendants implemented this scheme of conversion through two entities set up with similar names, Defendant CipherBlade LLC ("the Alaska Entity") and Defendant CipherBlade APAC PTE LTD ("the Singapore Entity"). Defendants misappropriated Plaintiff's trade secrets, information technology and other assets to transition Plaintiff's business and operations to these entities.

The temporary restraining order sought here is reasonable and necessary in view of the Defendants' takeover of Plaintiff's information technology infrastructure, their denial of system access to Plaintiff, and their material misrepresentations about Plaintiff and their credentials, expertise, and experience. In cases of an unlawful misappropriation of a domain and the associated information technology infrastructure, such as here, the relief sought to restore access and control to the domain and associated information technology infrastructure is properly granted as a temporary restraining order in order to return the parties to the status quo and to mitigate the severe irreparable harm resulting from being locked out of one's information technology systems.

II. FACTUAL BACKGROUND

A. Introduction

Richard Sanders first co-founded the company in the United Kingdom as CipherBlade Ltd. (hereinafter the "UK Entity"). Sanders Decl. ¶ 2. The business of CipherBlade was later transitioned to the United States in early 2021 and operated through CipherBlade PA. Sanders

Decl. ¶ 2. In 2019, Mr. Sanders hired Paul Sibenik to work at CipherBlade. Sanders Decl. ¶ 13; Sibenik Decl. ¶ 6. Mr. Sibenik transitioned to CipherBlade PA when it became operational in early 2021 and acted as the Lead Case Manager and the most senior full-time investigator at the company, testifying as well as an expert in cryptocurrency-related investigations and cases. Sanders Decl. ¶ 13; Sibenik Decl. ¶¶ 6, 9. Over time, Mr. Sanders expanded the scope of Mr. Sibenik's work to include overseeing more business and operational tasks. Sanders Decl. ¶ 13; Sibenik Decl. ¶ 10. On June 16, 2023, Mr. Sanders transitioned the role of CipherBlade PA CEO to Mr. Sibenik, a title he properly retains to this day. Sanders Decl. ¶ 14; Sibenik Decl. ¶ 11.

In or about May or June 2019, Manuel Kriz was hired at the UK Entity to work as an investigator, as well as to handle back-office related items such as invoices, business leads, general company email responses, engagement agreements and other contractual items (generation thereof – not signing), and client calls. Sanders Decl. ¶¶ 21-22. Mr. Kriz was ultimately responsible for some finance-related duties but did not have the authority to sign any documents on Mr. Sanders' behalf or make any critical decisions for CipherBlade PA. *Id.* at ¶ 22.

In mid-2021, Mr. Kriz told Mr. Sanders that he was hiring an additional individual, Mr. Michael Krause, in a limited capacity as a contractor, to assist with CipherBlade PA's daily tasks. Sanders Decl. ¶ 23. However, shortly thereafter, in late 2021/early 2022, Mr. Kriz advised Mr. Sanders that he required more assistance with his daily tasks and would be elevating Mr. Krause to a more substantial role. *Id.* at ¶ 24. Over time, Mr. Sanders came to trust Mr. Krause and gave him additional, limited authority, upon request, to take on further back-office duties, such as handling routine transactions and routine administrative functions, including payroll and licensing payments, about which Mr. Sanders would be made aware. *Id.* at ¶ 25. Ultimately, Mr. Krause grew into a trusted business colleague and friend to Mr. Sanders – or so Mr. Saunders was led to

believe. *Id.* at ¶¶ 23, 25.

In late 2022, Mr. Sanders sought to take a step back from the day-to-day operations of CipherBlade PA to volunteer in Ukraine, specifically to assist the National Police with cryptocurrency investigations. Sanders Decl. ¶ 26. In preparation for this process, he recognized that he required assistance managing the administrative, business management, and accounting tasks he typically oversaw. *Id*. at ¶ 27. To transition these duties, Mr. Sanders granted both Messrs. Kriz and Krause limited administrative access and authority to manage CipherBlade PA's IT infrastructure. *Id*. at ¶ 27. They were also authorized to retain others as needed. *Id*. at ¶ 27. In the leadup to Mr. Sanders eventual departure to Ukraine in February 2023, Mr. Kriz hired Mr. Krause's two sons, Jorn Henrik Bernhard Janssen and Paul Marnitz, as well as Ioana Vidrasan, in an assistant-like capacity. *Id*. at ¶ 28. Just after Mr. Sanders' departure to Ukraine, Messrs. Kriz and Krause also hired Justin Maile in March 2023 and Jussi Aittola in April 2023. *Id*. at ¶ 30. Both Mr. Maile and Mr. Aittola were former employees of Chainalysis, an important partner of Plaintiff. *Id*. at ¶ 30.

B. The Setup and Fraudulent Impersonation of Mr. Sanders and Plaintiff

As part of onboarding Messrs. Aittola and Maile, the Defendants represented to Mr. Sanders that setting up separate CipherBlade entities may be necessary to facilitate business opportunities and segregate business lines in the future. Sanders Decl. ¶ 31. Defendants then falsely represented to Mr. Sanders that the separate CipherBlade entities would be set up in Alaska and Singapore and each would be: (i) affiliated with CipherBlade PA, and (ii) registered as owned by Mr. Sanders. *Id*. This was not so. *Id*.. While Mr. Sanders consented – after much cajoling – to these new CipherBlade entities, subject to the conditions described, he did not know what actually happened. *Id*. It turns out that Mr. Maile created his own company, mimicking the name

"CipherBlade LLC," and incorporating it in Alaska, but not for Mr. Sanders' ("the Alaska Entity"). *Id*. at ¶ 32. Similarly, Mr. Aittola also created his own limited company in Singapore in his own name and not Mr. Sanders', CipherBlade APAC Pte Ltd ("the Singapore Entity"). *Id.* at ¶ 33. In truth, neither the Alaska Entity nor the Singapore Entity was associated with CipherBlade PA, unbeknownst to Mr. Sanders.

With the fraudulent corporate infrastructure in place, the Defendants, through misrepresentations, gained access to Mr. Sander's email and personal information which they used to impersonate him and cause irreparable harm to Plaintiff. Sanders Decl. ¶¶ 41-44. Immediately before Mr. Sanders went to Ukraine, he granted the Defendants limited authority to create and utilize a new email address, richard@cipherblade.com, for the sole purpose of digitally signing routine client engagements. *Id*. at ¶ 41. Defendants abused this email address, as discussed below.

Mr. Sanders also maintained another work email account, rich@cipherblade.com, which he used to manage key infrastructure within the business, including the domain name cipherblade.com, Google Workspaces, and other internal systems. Sanders Decl. ¶ 40. On several occasions, Defendants tried gaining access to Mr. Sanders' personal "rich@cipherblade.com" email but were unsuccessful. *Id. at* ¶ 42. For example, on January 31, 2023, while he was in Ukraine, Defendants solicited Mr. Sanders for access to the "rich@cipherblade.com" email account, which he did not provide. *Id. at* ¶ 43. Defendants repeatedly made these types of access requests, messaging Mr. Sanders to ask for direct access to his email claiming to require access to handle administrative tasks. *Id*. at ¶¶ 42-3.

While the Defendants could not gain access to the key rich@cipherblade.com email, over the next several months, they used the richard@cipherblade.com account to fraudulently communicate with others, falsely claiming to be on behalf of CipherBlade PA and Mr. Sanders

himself, causing substantial harm to CipherBlade PA and Mr. Sanders' personally. Sanders Decl. ¶ 41. They even used Mr. Sanders' email to give the illusion that their fraudulent scheme was at his direction and with his consent. *Id.* ¶¶ 50-51. For example, on or around April 18, 2023, Mr. Sanders directed Mr. Krause to send a termination notice to Mr. Kriz. *Id. at* ¶ 45. Mr. Krause used the "richard@cipherblade.com" email to do so instead of using his own email account, which Mr. Sanders found suspicious, due to the limited purpose for which that email account had been established. *Id.*

Defendants did not have authority to use the richard@cipherblade.com email account account in this way and the substance of the email was also suspicious. Sanders Decl. ¶ 45. Mr. Krause wanted Mr. Sanders to think that Mr. Kriz was terminated so Defendants could continue to execute their planned scheme. *Id. at* ¶ 48. In reality, Mr. Kriz was still working behind the scenes, accessing Google drives, and chatting on internal CipherBlade PA channels. *Id. at* ¶ 49.

Next, Defendants began contacting customers and contractors purportedly on behalf of Mr. Sanders, without his knowledge or authorization. Sanders Decl. ¶ 50. These emails went so far as to include a *picture* of Mr. Sanders on the signature line. *Id.* In one instance, on March 29, 2023, Defendants accessed Mr. Sanders' email and terminated an existing contractor agreement between Mr. Sibenik and CipherBlade PA to change a previously agreed upon revenue sharing structure. *Id. at* ¶ 51.

Even more concerning, the Defendants did not limit their theft and impersonation of Mr. Sanders to the digital world. Sanders Decl. ¶ 52. They also engaged in physical theft, breaking and entering, credit card fraud, and impersonation via the U.S. Postal Service. *Id.* While abroad in Ukraine, Mr. Sanders received a series of alerts from his home security system that indicated all of his security cameras suddenly went offline. *Id.* Upon returning home, Mr. Sanders found his

home ransacked and observed that business registration-related documents, including LLC and business filings, were missing. *Id. at* ¶ 53. After cleaning up his home and assessing the damage, he found a U.S. Postal Service receipt for a package mailed by U.S. Mail from his Pennsylvania home purportedly by him to an address in Cyprus at a time he was out of the country, fraudulently using his name, and credit card information without permission. *Id*. at ¶ 54.

C. The Theft of the CipherBlade.com Domain and CipherBlade PA's Essential Business Systems

CipherBlade PA uses Google Workspaces to issue and manage all email accounts associated with the cipherblade.com domain. Sibenik Decl. ¶ 32. Importantly, each user and email account may have different administrator rights depending on the privilege level associated with the account in Google Workspaces. *Id*. at ¶ 23. For example, the cipherblade.com domain, which Mr. Sanders registered with the U.S.-based domain registrar, Namecheap, Inc., could only be accessed by Mr. Sanders' personal work email account: rich@cipherblade.com email account, so no one other than Mr. Sanders himself was able to access the contents of his email account. Sanders Decl. ¶¶ 56-57; Sibenik Decl. ¶ 23. That Namecheap account also had two-factor authentication (2FA) implemented, meaning that Namecheap would send an additional secret code to Mr. Sanders' email account that was required to access the account. Sanders Decl. ¶ 56; Sibenik Decl. ¶ 24.

Critically, on May 4, 2023, four days after he was supposedly fired, Mr. Kriz set up a Google Meeting with HiView (a Google product reseller from which Plaintiff licensed its Google Workspace product) labelled "CipherBlade | HiView Workspace Sync." Sibenik Decl. ¶ 21. While Plaintiff is unaware of the specific discussion, it represents at least the beginning of a campaign to gain access and control over Plaintiff's entire information technology infrastructure, ultimately causing incalculable, irreparable harm to Plaintiff' business and reputation. *See Id*.

On June 13, 2023, Defendants temporarily disabled Mr. Sanders' authentic email account (rich@cipherblade.com), thereby removing Mr. Sanders access to his company's website, related services, and any communications sent to his email address. Sanders Decl. ¶¶ 59-60; Sibenik Decl. ¶¶ 24-25. This also prevented Mr. Sanders from receiving any email associated with the 2FA secret code from any Namecheap login attempt. Id. On information and belief, Defendants intercepted Mr. Sanders' email communications while they had disabled his account, likely by creating an unauthorized mail forwarding rule, so that they could acquire the 2FA secret code. *See* Sibenik Decl. ¶ 24. After gaining access to Mr. Sanders' Namecheap account, the Defendants changed the contact and account ownership information of the Namecheap account that was associated with cipherblade.com from rich@cipherblade.com to billing@cipherblade.com. Sanders Decl. ¶ 59; Sibenik Decl. ¶ 24. After Defendants completed the theft of the Namecheap account, that same day, June 13, 2023 Defendants restored Mr. Sanders' email. Sibenik Decl. ¶ 25.

Defendants could only have accessed the Namecheap account to make these changes by stealing access to Mr. Sanders' rich@cipherblade.com email messages without his authorization. Sanders Decl. ¶ 60. With the Namecheap account ownership now under the control of the Defendants-controlled billing@cipherblade.com email, the Defendants successfully stole control of the Namecheap account, thereby usurping control of all domain management functionality from CipherBlade PA. Sanders Decl. ¶¶ 59-61; Sibenik Decl. ¶ 23-25. Finally, at some point, on or before June 16, 2023, Defendants then demoted Mr. Sanders' from an Administrator level account to a normal user account, thereby removing Mr. Sanders' privileges to manage any account associated with the CipherBlade PA infrastructure, including the Defendants' accounts. Sibenik Decl. ¶¶ 21-22. Mr. Sanders was left with no administrative privileges whatsoever, and no ability to assess or control the Defendants' subsequent actions. *See Id*. at 22.

With this ultimate level of control achieved, the Defendants moved on to the next step of the domain takeover. On July 3, 2023, Plaintiff's counsel provided Defendants' counsel with a courtesy copy of the Complaint filed on June 30, 2023.The relief requested in the Complaint included the return of the cipherblade.com domain. That same day, July 3, 2023, Defendants utilized their illicit access to the stolen Namecheap account and transferred the domain from Namecheap, a U.S.-based registrar, to OVH SAS, a domain name registrar located in France. Sibenik Decl. ¶¶ 26-27. And, finally, on July 3, 2023, using their access, the Defendants altered the ownership information of the domain. *Id.* at ¶ 28. The Defendants changed the owner of the domain to "omega3zone Global Ltd." and changed the registrant country to Cyprus. *Id*. Upon further research, the Plaintiff discovered that omega3zone is a Cyprus-based company owned by Defendants Mr. Marnitz and Ms. Vidrasan, who were previously hired to be Mr. Sanders' assistants. *Id*. at ¶ 29.

Now that the Defendants had full control of the CipherBlade PA domain name, they took control of various IT infrastructure, essential business tools and functions, including the customer relationship management software platforms Lawmatics and Freshdesk, through several unauthorized administrative changes, as well as Defendants' continued abuse of administrative permissions, effectively wreaking havoc on Cipher Blade PA's ability to function as a business. Sibenik Decl. ¶ 30. The Defendants' access to the domain name also allowed them to take control of the domain name's web hosting account with Google, the customer relationship management (CRM) tools to respond to inbound inquiries, as well as the backend IT infrastructure that is hosted with Google Workspaces, which controls contractors' email access. *Id*. at ¶ 32. After gaining access to this infrastructure, the Defendants revoked access to CipherBlade PA IT infrastructure for Mr. Sanders as well as CipherBlade PA contractors not part of Defendants' conspiracy. *Id*. at

¶ 31.

Defendants have also converted Plaintiff's cloud assets including confidential and trade secret business and customer information on these computer systems, with the intent to steal clients and misappropriate client funds. Sibenik Decl. ¶¶ 30, 45. Now that Defendants have taken control of the CipherBlade PA domain name, its hosting, and the back-end IT infrastructure of the company, at this moment, CipherBlade PA is completely locked out of, and no longer has access to, important business generation data, customer contact information, and communications with customers. *Id*. at ¶ 60. This irreparably harms Plaintiff, and this harm grows each day Plaintiff is denied access to its IT infrastructure and the confidential information and trade secrets essential to Plaintiff's business. *Id*. at ¶ 60.

D. Defendants' Material Misrepresentations Have Caused, and Continues to Cause, Irreparable Harm to CipherBlade PA's Current and Future Business

By way of the above-described email and domain takeover, the Defendants have confused customers by making misrepresentations about CipherBlade PA's location in Pennsylvania, misrepresenting the skill and experience of their fraudulent Alaska Entity, changing the cost of services or underbidding Plaintiff with access to Plaintiff's pricing, and wrongfully converting CipherBlade PA customers to the Alaska Entity. Sibenik Decl. ¶¶ 39-40.

Defendants have used the converted domain and website to make false statements of material fact in advertising their services. Sibenik Decl. ¶ 33. This includes passing off the experience, expertise and tools of Plaintiff as their own. *Id*. at ¶¶ 33-34. The cipherblade.com website that they converted and now control falsely lists Mr. Sanders' personal professional certification as evidence of their Chainalysis certification. Further, the website lists various law firms as references that are in fact the references of Plaintiff CipherBlade PA (Mr. Sanders and Mr. Sibenik). *Id*. at ¶ 36. The website further contains sections entitled "Our Network" and "In the

Press," referencing articles concerning Plaintiff and Plaintiff's work prior to Defendants' takeover of the website and domain, including Mr. Sanders' and Mr. Sibenik's media and press appearances. *Id*. at ¶ 37. The CipherBlade website includes a blog with posts that Mr. Sibinek primarily wrote for Plaintiff, but Defendants have removed his name as author and now misleadingly list only 'CipherBlade' as the author. *Id*. at ¶ 38. The website also falsely makes claims about Defendants' experience that are, in fact, the experience of Plaintiff. See *Id*. at 35.

The commandeered website also states that Defendants have recovered millions of dollars of stolen cryptocurrency and have investigated and tracked Bitcoin belonging to suspects in hundreds of cybercrime cases. This is the experience of Plaintiff, not the Defendants. Finally, the website makes the false claim that "We have served as expert witnesses on major cases." This, once again, is Plaintiff's experience and not that of Defendants.

The Defendants also engaged in slanderous misrepresentations in an effort to capture existing CipherBlade PA clients. In June 2023, an active client messaged Mr. Sibenik questioning if he was separating from CipherBlade PA. Sibenik Decl. ¶¶ 41-42. The client forwarded a message from Defendant Sergio Garcia (who used the alias Miguel Alonso Torres) in which he represents that "CipherBlade has had to separate from its Pennsylvania unit, comprising Richard, Paul, and Sasha. . . ." *Id*. at ¶ 41. This message makes additional disparaging remarks about Mr. Sibenik, Mr. Sanders and another CipherBlade PA employee not involved in the scheme and requests that the client contact Defendant Garcia's CipherBlade email in the future. *Id*.

The Defendants also engaged in active outreach to clients, in which they fabricated detrimental and demeaning stories about Plaintiff. For example, on July 3, 2023, the Defendants reached out to an active client and stated "Regrettably, CipherBlade has had to separate from its Pennsylvania unit due to increasingly erratic and unconscionable behavior by representative of the

same, including threats of violence and other harm to multiple team members. . .” Sibenik Decl. ¶ 40. The Defendants go on to state that “[t]his has promoted the [independent] owner of the CipherBlade trademark to revoke the trademark license to CiherBlade LLC, Pennsylvania effective in less than 30 days.” *Id*. These allegations about Plaintiff and its representatives were simply untrue and were made maliciously to malign the reputation and the goodwill Plaintiff had built with customers and the community.[1] These are examples of recurring behavior in which Defendants have interfered with CipherBlade PA’s existing relationships and have caused it irreparable harm.

Defendants also began accepting payments that should have been received by Plaintiff. The clients who made these payments believed that Plaintiff would receive those funds. In July 2023, one CipherBlade PA client sent Defendants a communication on Telegram, a secure messaging app CipherBlade PA uses, explaining, “I don’t understand how we paid the wrong CipherBlade group when I specifically asked for Paul [Sibenik] and they said you don’t work for them anymore. This is very frustrating because I don’t know who to believe and y’all are from the same company.” Sibenik Decl. ¶ 49. As a result of Defendants’ misrepresentations, this client mistakenly paid the Alaska Entity $30,000 USD instead of CipherBlade PA, which they assumed they were engaging for work done by Paul Sibenik. *Id*. at ¶ 50.

The Defendants have also caused issues with CipherBlade PA’s attempt to engage with new clients. *See* Sibenik Decl. ¶ 47. For example, on June 5, 2023, CipherBlade PA entered into an Engagement Agreement with a potential client, a citizen of the United Kingdom, to perform

[1] The CipherBlade Trademark was registered on or about July 2022 by the CipherBlade UK entity at a time when the business using the CipherBlade trademark in U.S. commerce had been and was CipherBlade PA. The propriety of such registration and any purported license, assignment or license termination of the trademark is the subject of the expedited discovery sought here. Moreover, Plaintiff has received no notice of any assignment of the trademark or termination of any license.

investigative and expert services in the field of blockchain forensics and cryptocurrencies. The client tried to contact Mr. Sibenik at his paul@cipherblade.com email address; however, due to Defendants' fraudulent takeover and subsequent restriction of CipherBlade PA's employees' privileges, Mr. Sibenik no longer had access to his CipherBlade PA's email account. Defendants' subsequent misrepresentations and false narratives to the client led to the client's withdrawal of their engagement with CipherBlade PA on July 12, 2023. *Id*. at ¶ 47.

E. Defendants Siphoned Funds from Plaintiff Using Fraudulent Enterprises and Causing Plaintiff Financial Harm

In 2022, as Mr. Sanders prepared for his trip to Ukraine, he entrusted Mr. Kriz and Mr. Krause with handling routine transactions on behalf of CipherBlade PA, which required him to give the Defendants access to CipherBlade PA's financial accounts with the money transfer company Wise. *See* Sanders Decl. ¶ 27 Sibenik Decl. ¶ 51. Unfortunately, the Defendants abused this access to siphon and misappropriate CipherBlade PA funds to the fraudulent CipherBlade enterprises they established. Sibenik Decl. ¶¶ 53-56. For example, upon review of CipherBlade PA's financial records, it was discovered that in 2023, after Mr. Sanders departed for Ukraine, the Defendants transferred $24,700 USD to the Singapore Entity. Sibenik Decl ¶ 58. The Defendants also created fraudulent shell companies to which they diverted Plaintiff's funds by disguising large payments as consulting or advisory fees. CipherBlade PA does not pay for any consulting or advisory services. *Id*. at ¶ 52. However, upon review of CipherBlade PA's financial records, several transactions to unknown companies that appear to be consulting or advisory service companies, were discovered. *Id*. at ¶ 53. CipherBlade PA discovered that in April 2023, $110,230.09 (USD) and €245,675.91 (EUR) was transferred from CipherBlade PA to Inquisita Solutions, a Cyprus-based company, which is owned by Mr. Kriz and Mr. Janssen. *Id*. at ¶ 54. As another example, CipherBlade PA discovered that in 2022, $119,502.60 was transferred from

CipherBlade PA to an entity entitled White Orchard Ltd. *Id*. at ¶ 55. Upon further research, Plaintiff discovered that White Orchard is owned by Defendant Manuel Kriz and is registered in Cyprus. The Defendants also used CipherBlade PA business accounts to pay Green Stone Business Advisory FZ LLC $435,199.59 (USD) in 2022, and $716,342.85 (USD) in 2023. Sibenik Decl ¶ 57. CipherBlade has never engaged services of this entity. *Id.*

As of this filing, Plaintiff believes Defendants wrongfully transferred at least $1,405,975.13 (USD) and €245,675.91 (EUR - approximately $276,131.86) to Green Stone, White Orchard Ltd., the Singapore Entity, and Inquisita Solutions.

Defendants also solicited payments from numerous current CipherBlade PA clients to the Alaska Entity. Sibenik Decl. ¶ 42. Because the CipherBlade PA employees who are not part of Defendants' conspiracy do not have visibility into client emails (because Defendants have locked them out of email access), it is currently impossible to know the full extent of the harm done. Mr. Kriz also encouraged multiple CipherBlade PA staff members who were contractors to send invoices for large bonuses to be paid by CipherBlade PA, in an attempt to curry favor with them, days before the Defendants fraudulently assigned their contractor agreements to the Alaska Entity. *Id*. at ¶ 44.

III. LEGAL STANDARDS

A temporary restraining order is an equitable remedy and an act of discretion by the court. *Am. Civil Liberties Union v. Clapper*, 804 F.3d 617, 622 (2d Cir. 2015). "In general, a party seeking a preliminary injunction or temporary restraining order 'must . . . show a likelihood of success on the merits, a likelihood of irreparable harm in the absence of preliminary relief, that the balance of equities tips in the party's favor, and that an injunction is in the public interest.'" *Coronel v. Decker,* 449 F. Supp. 3d 274, 280–81 (S.D.N.Y. 2020). Plaintiff meets all of these factors. Plaintiff will likely succeed on the merits because the facts demonstrate clear theft and

impersonation, which is causing and will continue to cause irreparable harm to Plaintiff and the public if the Defendants continue to operate using Plaintiff's assets, including its information technology infrastructure, confidential information and trade secrets. Nor can Defendants demonstrate that any ***legitimate*** interests of Defendants will be harmed, and the effect on third parties (such as clients) with whom Defendants have made illegal contracts will be negligible and temporary. Accordingly, the relief Plaintiff request is warranted.

A. Defendants Have Caused Irreparable Harm to the Plaintiff

Defendants' conduct has caused and threatens to cause significant and irreparable harm to Plaintiff. A TRO is appropriate where, as here, a plaintiff is threatened with potential harm "that cannot be remedied if a court waits until the end of a trial to resolve the harm." *Grand River Enter. Six Nations, Ltd. v. Pryor*, 481 F.3d 60, 66 (2d Cir. 2007) (internal citations omitted).

First and foremost, Plaintiff's loss of its trade secrets, confidential information, and digital assets, cause irreparable harm. Irreparable harm is presumed where a trade secret has been misappropriated because, in the words of the Second Circuit, "[a] trade secret once lost is, of course, lost forever" and, Defendants' use of that information put Plaintiff at a competitive disadvantage that a legal remedy cannot address. *FMC Corp. v. Taiwan Tainan Giant Indus. Co.*, 730 F.2d 61, 63 (2d Cir. 1984); *Secured Worldwide LLC v. Kinney,* No. 15 Civ. 1761 (CM), 2015 WL 1514738, at *11 (S.D.N.Y. Apr. 1, 2015); *Estee Lauder Cos. Inc. v. Batra*, 430 F. Supp. 2d 158, 174 (S.D.N.Y. 2006). For a preliminary injunction, loss of trade secrets is considered irreparable harm. *See Comput. Assocs. Int'l., Inc. v. Bryan*, 784 F. Supp. 982, 986 (E.D.N.Y. 1992).

Defendants also continue to engage in false advertising, through the use of CipherBlade's website and email, by claiming Plaintiff company, experiences, accolades. A Lanham Act plaintiff "who can prove actual lost sales may obtain an injunction even if most of his sales decline is

attributable to factors other than a competitor's false advertising" in fact "he need not even point to an actual loss or diversion of sales." *Coca-Cola Co. v. Tropicana Prods., Inc.,* 690 F.2d 312, 316 (2d Cir. 1982) (internal citations omitted). "In order to succeed on the merits of a false advertising claim under the Lanham Act, a party must show either literal falsity of the advertising under scrutiny or that the advertising is literally true but likely to mislead or confuse." *SQP, Inc. v. Sirrom Sales, Inc.*, 130 F. Supp. 2d 364, 366 (N.D.N.Y. 2001) (citing *McNeilab, Inc. v. Am. Home Prods. Corp.,* 848 F.2d 34, 38 (2d Cir.1988)). Defendants' use of the website and claiming the experience and accolades of CipherBlade PA is patently false, or at least likely to mislead or confuse. For example, the website lists various law firms as references that are in fact the references of Plaintiff CipherBlade PA (Mr. Sanders and Mr. Sibenik). The website also lists "Our Network" and "In the Press," referencing articles concerning Plaintiff and Plaintiff's work prior to Defendants' takeover of the website and domain, including Mr. Sanders' and Mr. Sibenik's media and press appearances. Complaint 100. Neither of those things are attributable to the Alaska entity which now controls the website. Those claims are about CipherBlade PA. In this case, Plaintiff has countless examples of evidence creating more than a mere subjective belief that the Plaintiff will be injured, including messages of concern from current and potential clients, including canceling of at least one contract because of this confusion. Sibenik Decl. ¶ 47.

Defendants continue to make material misrepresentations to current and potential customers. Here, Defendants misconduct injures CipherBlade PA's goodwill, creating confusion about the source of CipherBlade PA's services, and damaging the reputation of and confidence in Plaintiff' services. Customers may migrate to other platforms, products, or services should they have problems contacting or working with Plaintiff because Defendants have taken control of Plaintiff's IT infrastructure and its confidential business information and trade secrets stored on its

systems. Once such a switch occurs, it is unlikely those customers will return to Plaintiff. These injuries constitute irreparable harm. *See Two Hands IP LLC v. Two Hands Am., Inc.*, 563 F. Supp. 3d 290, 307 (S.D.N.Y. 2021); *Ecolab Inc. v. Paolo*, 753 F. Supp. 1100, 1110 (E.D.N.Y. 1991); *see also Tom Doherty Assocs., Inc. v. Saban Ent., Inc.,* 60 F.3d 27, 37-38 (2d Cir. 1995); *Broker Genius, Inc. v. Volpone*, 313 F. Supp. 3d 484, 496 (S.D.N.Y. 2018).

Courts have found risk of irreparable harm in matters concerning fraudulent transfers of cryptocurrency "due to the risk of anonymous and speedy asset dissipation" *See Jacobo v. Doe,* No. 1:22-cv-00672-DAD-BAK (BAM), 2022 WL 2052637, at *5 (E.D. Cal. June 7, 2022)*; see also Fed. Trade Comm'n. v. Dluca*, No. 18-60379-CIV-MOORE/SNOW, 2018 WL 1830800, at *2 (S.D. Fla. Feb. 28, 2018), *report and recommendation adopted*, No. 0:18-CV-60379-KMM, 2018 WL 1811904 (S.D. Fla. Mar. 12, 2018) (Plaintiff is likely to suffer immediate and irreparable harm without injunctive relief because defendant could transfer cryptocurrency to outside the traditional banking system so the assets are beyond the reach of the court.).

If Defendants retain Plaintiff' trade secrets, confidential information, access to financial accounts, including cryptocurrency assets, and proprietary information because they are not enjoined, Plaintiff faces significant and irreparable harm. It is exceedingly difficult, if not impossible, to predict Plaintiff's loss if Defendants are permitted to retain, distribute, and exploit such information. If Defendants are allowed to proceed with their unlawful misconduct unrestrained, then Defendants may succeed in undermining Plaintiff's business and goodwill, causing substantial irreparable and incalculable harm. Only by immediately enjoining Defendants from acquiring, disclosing, or using Plaintiff' Trade Secrets, Confidential Information, and Digital Assets will ensure that Defendants will not cause any further irreparable damage to Plaintiff's business. Therefore, a finding of irreparable harm and an emergency injunction are appropriate.

B. Plaintiff Are Likely to Succeed on the Merits

Here, Plaintiff are likely to succeed on the merits of all of its claims given the direct evidence it has already gathered definitively showing Defendants' trade secret misappropriation, conversion, and violation of the Lanham Act. The evidence available establishes a *prima facie* claim under the DTSA. The elements of Plaintiff' trade secret misappropriation claim and conversion claim, turn on substantially the same facts because the misappropriation and conversion were accomplished by improperly obtaining control of Plaintiff's assets, including its IT infrastructure and all the confidential information and trade secrets contained therein. In evaluating the likelihood of success, a plaintiff "need not show that success is certain, only that the probability of prevailing is 'better than fifty percent,'" meaning a court need not determine that movants "*have* succeeded on the merits to issue an injunction. It need only decide that they *likely may*." *Greenlight Cap., L.P. v. Apple, Inc.*, Nos. 13 Civ. 900 (RJS), 13 Civ. 976 (RJS), 2013 WL 646547, at *4 (S.D.N.Y. Feb. 22, 2013). Plaintiff meets this standard.

1. Defendants' Theft of CipherBlades PA's Trade Secrets

To prevail on a claim for misappropriation under the Defend Trade Secrets Act ("DTSA"), a plaintiff must demonstrate (1) the existence of a trade secret, which is defined as information that has derived "independent economic value" from being kept secret, is "related to a product or service used in, or intended for use in, interstate or foreign commerce," and (3) the misappropriation of that trade secret, which is defined as knowingly acquiring a trade secret through improper means. 18 U.S.C. § 1836.

As discussed above, Defendants took control of CipherBlade PA's IT infrastructure, made various unauthorized administrative changes, and abused various administrative permissions, thereby blocking Plaintiff from access to its own proprietary business information. Sibenik Decl.

¶ 30. Defendants initiated account takeovers over many different assets, including, most notably, the CipherBlade PA domain name (cipherblade.com). Sibenik Decl. ¶¶ 23-24, 32. Taking over the CipherBlade PA domain allowed Defendants to also take control of the hosting infrastructure with Google and Google Workspaces, which provides employees with email access, as well as backend access to countless tools needed to function the business. Sibenik Decl. ¶¶ 21-22. Defendants have continued to make use of and access CipherBlade PA's confidential information, IT infrastructure, and proprietary customer information – the very type of activities the DTSA was enacted to protect against.

2. Lanham Act

Plaintiff has established a likelihood of success in proving that Defendants' conduct violates the Lanham Act § 1125(a). Section 1125(a) states that "any person who, on or in connection with . . . services. . . uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which . . . (A) is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services. . . "shall be liable in a civil action . . ." 15 U.S.C.A. § 1125 (a)(1).

In carrying out their scheme, Defendants rely on the use of Plaintiff' logo and website, containing false and misleading statements about their services. Defendants also have used these misrepresentations and CipherBlades PA's website, email systems, and infrastructure to mislead customers and vendors into signing agreements with CipherBlade Alaska and CipherBlade Singapore. Sibenik Decl. ¶ 41. Primarily, the Defendants use Plaintiff's website to make false statements of material fact about their services, including their experience, expertise and tools,

which should be attributed to CipherBlade PA. The Defendants abuse their fraudulent access to the cipherblade.com website and corresponding logo to falsely claim they are the CipherBlade entity responsible for all of the certificates and accolades on the website, confusing and luring in customers, when the truth is, the Defendants have none of that knowledge or experience.

Defendants have also used access to CipherBlade's logo and representation to fraudulently contract with clients and potential clients. Because users cannot discern that they are contracting with Defendants, they mistakenly believe that they are dealing with the products and services of CipherBlade PA. Sibenik Decl. ¶ 41. Similarly, users and even sophisticated security industry consumers are unable to discern between Plaintiff, on one hand, and the Alaska Entity and Singapore Entity, on the other hand, especially as emails from Defendants are sent using the CipherBlade PA logo and Mr. Sanders' picture, meaning that clients will mistakenly believe they are getting Plaintiff and its experience, expertise and investigative tools when they are being deceived into purchasing the services of Defendants.

3. Trespass to Chattels & Conversion

A trespass to chattels occurs where a defendant intentionally and without justification or consent, interferes with the use and enjoyment of personal property in the plaintiff's possession and, as a result, causes damages. *Sch. of Visual Arts v Kuprewicz,* 3 Misc. 3d 278, 281 (2003); *Yo! Braces Orthodontics, PLLC v. Theordorou,* No. 602866/09, 2011 N.Y. Misc. LEXIS 1820, *8 (Apr. 19, 2011). Conversion occurs where a defendant makes an unauthorized assumption and exercise of the right of ownership over goods belonging to another, to the exclusion of the owner's rights. *Thyroff v. Nationwide Mut. Ins. Co.,* 8 N.Y.3d 283, 284, 288-89 (2007).

Defendants have done both by interfering with and taking as their own Plaintiff' resources. Defendants perpetrated several account takeovers in the days leading up to their final takeover date. This includes many things, but most notably the CipherBlade PA domain. Sibenik Decl. ¶

24) which was moved abroad. Defendants have also taken over the hosting infrastructure with Google and Google Workspaces, which grants employees email access. Sibenik Decl. ¶ 22. Having administrative access and control over this infrastructure in turn allowed for control over access (including the ability to revoke access) for additional CipherBlade PA IT infrastructure. Sibenik Decl. ¶ 22. Defendants also have made unauthorized payments to themselves as purported vendors and asserted control over some of CipherBlade's PA's cryptocurrency assets. Sibenik Decl. ¶ 52. For example, Defendants transferred CipherBlade PA funds in a series of transactions captured as "Management Services" and "Consulting." Sibenik Decl. ¶ 53. These payments were made shell companies, such as Inquisita Solutions Ltd in the amount of $110,230.09 (USD) and €245,675.91 (EUR). These transfers were made from CipherBlade's PA's business accounts. According to corporation records, Inquisita Solutions Ltd.'s Director and Secretary are listed as Defendants Mr. Kriz and Mr. Janssen. The Defendants also used CipherBlade PA business accounts to pay Green Stone Business Advisory FZ LLC $435,199.59 (USD) in 2022, and $716,342.85 (USD) in 2023. CipherBlade has never engaged services of this entity. Sibenik Decl. ¶ 57.

These activities injure the value of Plaintiff' property and result in unauthorized intrusion into those computers and theft of information, account credentials, and funds. These circumstances constitute trespass to chattel and warrant issuance of a TRO. *See Sch. of Visual. Arts,* 3 Misc. 3d at 282 (sending unsolicited bulk email states a claim for trespass to chattels where processing power and disk space were adversely affected); *see also Physicians Interactive v. Lathian Sys.,* No. CA-03-1193-A, 2003 U.S. Dist. LEXIS 22868, at *25, 31 (E.D. Va. Dec. 5, 2003) (TRO and preliminary injunction where defendant hacked computers and obtained proprietary information). Accordingly, Plaintiff are likely to succeed on their trespass to chattel and conversion claims.

C. The Balance of Hardships Tips Sharply in Plaintiff's Favor

Defendants will suffer no harm to any legitimate interest if a TRO is granted. CipherBlade

PA seeks relief to limit the irreparable harm it faces daily from being locked out of its business, the misappropriation of and denial of access to its confidential proprietary information, and the diversion of customers and leads. Because Defendants are engaged in an illegal scheme to defraud consumers and injure Plaintiff, the balance of equities tips in favor of granting a restraining order. *See, e.g., N. Atl. Operating Co., Inc. v. Evergreen Distribs., LLC*, No. 13-CV-4974 (ERK)(VMS), 2013 WL 5603602, at *13 (E.D.N.Y. Sept. 27, 2013) ("Where the only hardship to Defendant from [an] injunction would be to prevent him from engaging in further illegal activity, the balance clearly weighs in Plaintiffs' favor.") (internal quotations omitted).

D. The Public Interest Favors a TRO

Every day that passes, Defendants confuse more customers and reap more money from their misdeeds. And the public interest is clearly served by enforcing statutes designed to protect the public, such as the Defend Trade Secrets Act and the Lanham Act. *See Syntel Sterling Best Shores Mauritius Ltd. v. The TriZetto Grp., Inc.,* 15 CIV. 211 (LGS), 2021 WL 1553926, at *13 (S.D.N.Y. Apr. 20, 2021), *aff'd in part, vacated in part, remanded, Syntel Sterling Best Shores Mauritius Ltd. v. The TriZetto Grp., Inc.*, 68 F.4th 792 (2d Cir. 2023) (finding that an injunction is in the public interest because "it upholds the law that protects [Plaintiffs] trade secrets . . . rights, and thus encourage future investment in innovation"); *see also ProFitness Phys. Therapy Ctr. v. Pro-Fit Ortho. & Sports Phys. Therapy P.C.*, 314 F.3d 62, 68 (2d Cir. 2002); *Intertek Testing Servs., N.A.,* Also, enforcing Defendants' legal obligations to Plaintiff is in the public interest. *See Sanofi-Synthelabo v. Apotex Inc.*, 488 F. Supp. 2d 317, 345-46 (S.D.N.Y. 2006); *Intertek Testing Servs., N.A, Inc. v. Pennisi*, 2020 WL 1129773 (E.D.N.Y. Mar. 9, 2020).

E. The TRO is Reasonable, Necessary and in Conformity with Law

The requested relief, which to protect Plaintiff's trade secrets and confidential information, is reasonable and lawful in scope. Courts have confronted requests for injunctive relief targeted at

disabling and transferring back domain names and websites which are being used inappropriately. *DISH Network L.L.C. v. Kumar*, 21-CV-6730 (JPO), 2022 WL 5108085, at *4 (S.D.N.Y. Oct. 4, 2022) (granting a injunctive relief and finding that Defendants operating a pirated TV website must disable the domains, make them inactive and non-transferable, and at the direction of the Plaintiff, transfer those domain names to the Plaintiff); *see also C.D.S., Inc. v. Zetler,* 298 F. Supp. 3d 727, 774 (S.D.N.Y. 2018) (ordering Defendants to transfer business domain names back to the Plaintiff, who had registered and paid for said domain names, after converting them to Defendants name during a business dispute); *Vogster Ent., L.L.C. v. Mostovoy*, 09-CV-1036 RRM/RER, 2009 WL 691215, at 6-7 (E.D.N.Y. Mar. 16, 2009) (granting injunctive relief and restricting Defendants access to domain names that Defendant registered, as part of his employment when they were not returned upon Defendants employment separation.) In each of the foregoing cases, the courts granted as a remedy the transfer of domains to Plaintiff's control, and away from the control of Defendants. Such relief is not prohibited by any statute or rule of law, is appropriate and necessary, and within the Court's broad equitable authority to craft remedies to prevent irreparable harm. Returning control of the misappropriated trade secrets and domain is within this Court's powers.

One of the goals of an emergency injunction is to maintain the *status quo*, defined as "the last actual, peaceable, noncontested status which preceded the pending controversy." *N. Am. Soccer League, LLC v. U.S. Soccer Fed'n, Inc,* 883 F. 3d 32, 36-7 (2nd Cir. 2018) (citing *Mastrio v. Sebelius*, 768 F.3d 116, 120 (2d Cir. 2014) (internal quotes omitted)). CipherBlade PA seeks to preserve the *status quo* by preventing any further misappropriation of its trade secrets, confidential information and digital assets, by returning access to Plaintiff, and to enjoin defendants from making materially false representations about their services or Plaintiff's services, including by misrepresenting the experience, expertise and investigative tools of Plaintiff as their own, all or

which has confused and will continue to confuse clients and the marketplace if not enjoined. As explained above, all four factors are satisfied.

F. Expedited Discovery Should Be Ordered

In order to present the facts of this case to the Court as completely as possible for purposes of a forthcoming motion for a preliminary injunction, and to discover the full extent of Defendants' unlawful activities and the corresponding damage done to CipherBlade PA, Plaintiff must conduct expedited discovery. *See U.S. Commodity Futures Trading Comm'n. v. CTI Group, LLC*, 12 CV 3754, 2012 WL 2924386, at *5 (S.D.N.Y. May 18, 2012). Specifically, Plaintiff seeks to serve narrowly focused interrogatories and request for production of documents, and to conduct depositions of Defendants to uncover relevant facts one five specific topics: (1) the extent of the Defendants access to Plaintiff's IT infrastructure and its confidential information and trade secrets contained therein and the use made of such infrastructure, confidential information and trade secrets; (2) the extent of Defendants use of such information technology, infrastructure, systems and accounts including the use or disclosure of proprietary client, matter and pricing and investigative information on such infrastructure, systems and accounts; (3) the extent of Defendants contact with clients and potential clients of Plaintiff and the statements made to them or in advertising about their experience, expertise, investigative tools or services or about Plaintiff; (4) the extent of Defendants misappropriation of funds to fraudulent entities and shell companies; and (5) the purported ownership, registration, or assignment of the CipherBlade trademark, and any license or termination of such mark. Plaintiff also seeks leave to serve third-party subpoenas to uncover the extent of the misrepresentations made to its commercial partners. This expedited discovery is reasonable, feasible and relevant to the resolution of the motion for preliminary injunction.

G. A Preservation Order Should Issue

So that the Court may effectively and completely evaluate the evidence relevant to this matter, Plaintiff also seeks an order requiring the parties to preserve all evidence relevant to the facts and circumstances alleged in Plaintiff's Complaint. This includes, but is not limited to, hard copy and electronic files, documents, data, electronic mail, instant messages, and text messages in the parties' possession, custody, or control relevant to the issues set forth in the Complaint. Preservations orders "are increasingly routine in cases involving electronic evidence, such as e-mails and other forms of electronic communication." *Treppel v. Biovail Corp.,* 233 F.R.D. 363, 370 (S.D.N.Y. 2006) (internal citation omitted). When evaluating preservation order requests, courts consider the danger of destruction absent a court order, whether any irreparable harm is likely to result to the party seeking preservation in the absence of an order, and the burden of preserving the evidence. *Id.*

In this case, such an order will ensure that the Court has all necessary information available as it considers Plaintiff's claims and the irreparable harm and damage Plaintiff has suffered and continues to suffer as a result of Defendant's unlawful acts. Such an order is particularly warranted and important here given Defendant's history of deleting chats and messages related to this matter, as well as Defendants propensity to use technology to move and hide misappropriated funds such that Plaintiffs will continue to be harmed in the absence of an order. Additionally, the burden of preserving the evidence falls entirely on the Defendants, as they have usurped control of the systems needed to preserve such evidence.

IV. Alternative Service

Counsel for Defendants CipherBlade, LLC (Alaska) and Mr. Justin Maile has agreed to accept service on their behalf. Because several of the Defendants are not located in the United States, Plaintiff requests that the Court order alternative service methods on those Defendants.

Rule 4(f)(3) provides that service on a foreign litigant can be effected "by other means not prohibited by international agreement, as the court orders." Nothing in Rule 4(f) "suggests that a court must always require a litigant to first exhaust the potential for service under the Hague Convention for parties in signatory countries like Cyprus or Belgium before granting an order permitting alternative service under Rule 4(f)(3). *In re GLG Life Tech Corp. Sec. Litig.,* 287 F.R.D. 262, 266 (S.D.N.Y. 2012). As for the entities based in the United Arab Emirates ("UAE") and Singapore, both countries are not signatories to the Hague Convention. This court has found that for both Singapore and the UAE, there is no international agreement that prohibits service via email. *In re One Apus Container Ship Incident on Nov. 30, 2022,* No. 22 Md. 3028 (PAE), 2022 WL 17370122, at *4 (S.D.N.Y. Dec. 2, 2022); *CKR L. LLP v. Anderson Invs. Int'l., LLC*, 525 F. Supp. 3d 518, 524 (S.D.N.Y. 2021).

Plaintiff requests that this Court order as set forth in the proposed Order to Show Cause that Defendants not represented by counsel who has agreed to accept service may be served by email to effect timely service to participate in the preliminary injunction proceedings and because Defendants have active email addresses known to Plaintiff and reasonably calculated to achieve actual notice of these proceedings. *See Zanghi v. Ritella*, No. 19-CV-5830, 2020 WL 589409, at *6 (S.D.N.Y. Feb. 5, 2020) ("The Hague Convention does not prohibit ... service by email.") This Court has repeatedly found that email service comports with due process. *See Group One Ltd. v. GTE GmbH,* 523 F. Supp. 3d 323, 345 (E.D.N.Y. 2021); *see also Pearson Educ. Inc. v. Doe 1*, No. 18-CV-7380, 2019 WL 6498305, at *3 (S.D.N.Y. Dec. 2, 2019); s*ee also Philip Morris USA Inc. v. Veles Ltd.*, No. 06-CV-2988, 2007 WL 725412, at *3 (S.D.N.Y. Mar. 12, 2007).

V. Conclusion

For the reasons stated herein and in papers submitted in support, the relief sought in the proposed Order to Show Cause should be granted.

Dated: July 20, 2023

Respectfully submitted,

s/Alexander J. Urbelis

Alexander Joseph Urbelis
Anne Li
James K. Stronski
Richard J. Stella III

CROWELL & MORING LLP
590 Madison Avenue, 20th Floor
New York, NY 10022
Telephone: (212) 223-4000
Fax: (212) 223-4134

Garylene Javier (*pro hac vice pending*)
CROWELL & MORING LLP
1001 Pennsylvania Avenue NW
Washington DC 20004-2595
Telephone: (202) 624-2500
Fax: (202) 628-5116
gjavier@crowell.com

Attorneys for CipherBlade, LLC.